



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/553,067	07/10/2007	Ravindra Waman Shevade	DYOU32.001APC	5517

20995 7590 09/02/2010  
KNOBBE MARTENS OLSON & BEAR LLP  
2040 MAIN STREET  
FOURTEENTH FLOOR  
IRVINE, CA 92614

EXAMINER
----------

RAHMAN, MAHFUZUR

ART UNIT	PAPER NUMBER
----------	--------------

2438

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

09/02/2010

ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

jcartee@kmob.com  
efiling@kmob.com  
eOAPilot@kmob.com

<b>Office Action Summary</b>	<b>Application No.</b> 10/553,067	<b>Applicant(s)</b> SHEVADE, RAVINDRA WAMAN	
	<b>Examiner</b> MAHFUZUR RAHMAN	<b>Art Unit</b> 2438	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 10 July 2007.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-32 and 34 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-32 and 34 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 10/11/2005 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All    b) ☐ Some \*    c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |                                                                                        |                                                                   |
|----------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)            | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948)    | Paper No(s)/Mail Date. _____                                      |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>10/11/2005, 03/06/2006</u> .                                  | 6) <input type="checkbox"/> Other: _____                          |

### **DETAILED ACTION**

Applicant's amendment filed on 10/11/2005 is acknowledged. Claims 33 and 35-36 have been cancelled. Claims 1-32 and 34 have been amended. Claims 1-32 and 34 are examined and pending.

#### ***Information Disclosure Statement***

The information disclosure statement (IDS) submitted on 10/11/2005 and 03/06/2006 has been considered. The submission is in compliance with the provisions of 37 CFR 1.97. Form PTO-1449 is signed and attached hereto.

#### ***Oath/Declaration***

The Oath/Declaration filed on 07/10/2007 is accepted by the examiner.

#### ***Drawings***

The drawings filed on 10/11/2005 are accepted by the examiner.

#### ***Priority***

The application is filed on 07/10/2007 and this is a 371 of PCT/GB04/01549 filed on 04/08/2004.

***Claim Objections***

1. Claim 15 is objected to because of the following informalities: claim 15 recites limitations “the super hash value” lack antecedent basis in the claim. Appropriate correction is required.

***Claim Rejections - 35 USC § 101***

2. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 31 and 32 is rejected under 35 U.S.C. 101 as being non statutory. Claims 31 and 32 recite “a computer readable medium having a program for executing a method of distributing/authenticating documents ...” but Applicant’s Specification defines the term medium as a data transmission (See, specifications, Paragraph 0096: computer program providing such software control and a transmission, storage or other medium by which such a computer program is provided). Pending claims are interpreted as broadly as their terms reasonably allow (See In re Zletz, 893 F.2d 3 19 (Fed. Cir. 1989)). The broadest reasonable interpretation of a claim drawn to a computer readable medium typically covers forms of non-transitory tangible media and transitory propagating signals per se in view of the ordinary and customary meaning of computer readable media (See *MPEP 2111.01*). When the broadest reasonable

Art Unit: 2438

interpretation of a claim covers a signal per se, the claim must be rejected under 35 U.S.C. §101 as covering non-statutory subject matter. See In re Nuijten, 500 F.3d 1346, 1356-57 (Fed. Cir. 2007) (transitory embodiments are not directed to statutory subject matter).

The Examiner suggests that a claim drawn to such a computer usable medium that covers both transitory and non-transitory embodiments may be amended to narrow the claim to cover only statutory embodiments to avoid a rejection under 35 U.S.C. §101 by adding the limitation "non-transitory" to the claim. Such an amendment would typically not raise the issue of new matter, even when the specification is silent because the broadest reasonable interpretation relies on the ordinary and customary meaning that includes signals per se. The limited situations in which such an amendment could raise issues of new matter occur, for example, when the specification does not support a non-transitory embodiment because a signal per se is the only viable embodiment such that the amended claim is impermissibly broadened beyond the supporting disclosure. See, e.g., Gentqv Galleiy, Inc. v. Berkline Corp., 134 F.3d 1473 (Fed. Cir. 1998).

### ***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

Art Unit: 2438

e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

**5. Claims 12, 14, 16, 18, 28, and 31 are rejected under 35 U.S.C. 102(e) as being anticipated by Matsumoto et al. (US 2003/0159048 A1, hereinafter, Matsumoto).**

**Regarding claim 12,** Matsumoto discloses a document distribution device for distributing a document to a recipient data processing apparatus via a data communications network, the document distribution device comprising

a data processing apparatus configured to process applications software for generating an electronic document (Paragraph 0066: document preparation software installed in a terminal device at a client site, and therefore time information for certification can easily and automatically be stamped on each document during preparation of the document), and

generate an original hash value from the electronic document (Paragraph 0014: a digest value computing means for computing a digest value including a hash value as a unidirectional function value based on a read document); and

a communication interface configured to communicate the original hash value to a recipient data processing apparatus before a predetermined event via a data communications network (Paragraph 0014: a transmitting means for correlating the digest value to an ID number of the client electronic document preparation terminal

Art Unit: 2438

device and transmitting the digest value and the ID number to the external organization device; Paragraph 0060: an offline verification may automatically be performed before online verification wherein a request for verification of the time stamps for the document digest value (TS-obj, H-doc), time information (TS-obj, T-fix), and the electronic signatures (TS-obj, SIG-2) is sent to the time stamp verification server 13 at the center), and

after the predetermined event, to communicate the electronic document to the recipient data processing apparatus via the data communications network (Abstract: the document preparation terminal device 30 transmits the prepared document; Paragraph 0014: based on the configuration where a digest value generated based on an electronic document prepared by a client electronic document preparation terminal device with electronic document preparation software incorporated therein is transmitted to an external organization device and the external organization device assigns the time of receipt and an electronic signature to the digest value and returns it to the client).

**Regarding claim 14**, Matsumoto discloses the document distribution device as claimed in claim 12, wherein the data processing apparatus is configured to encrypt the original hash value using a private key associated with the document distribution device (Paragraph 0048: hash value is a value computed through a hash function which is a unidirectional function wherein the hash function used for encryption; Paragraph 0039: Secret key for generation of a signature).

**Regarding claim 16**, Matsumoto discloses the document distribution device as claimed in claim 12, wherein the data processing apparatus is configured to encrypt the electronic file containing the document produced by the applications software using the private key associated with the document distribution device prior to being communicated to the recipient data processing apparatus (Paragraph 0048: hash value is a value computed through a hash function which is a unidirectional function wherein the hash function used for encryption; Paragraph 0039: Secret key for generation of a signature).

**Regarding claim 18**, Matsumoto discloses the document distribution device as claimed in claim 12, wherein the applications software provides an on-line web browser, wherein the document is generated from the on-line browser, and wherein the data communications network includes at least one of an intranet and the Internet (Matsumoto Paragraph 0044: The time stamp processing center 10 and the electronic document preparing organization 20 are connected through a communication network 50 such as the Internet to each other so that communications can be performed therebetween) .

**Regarding claim 28**, Matsumoto discloses a method for distributing documents to a recipient data processing device via a data communications network, the method comprising:

generating an electronic document (Paragraph 0066: document preparation software installed in a terminal device at a client site, and therefore time information for



Art Unit: 2438

certification can easily and automatically be stamped on each document during preparation of the document);

generating an original hash value from the electronic document (Paragraph 0014: a digest value computing means for computing a digest value including a hash value as a unidirectional function value based on a read document); and

communicating the original hash value to a recipient data processing apparatus before a predetermined event via a data communications network (Paragraph 0014: a transmitting means for correlating the digest value to an ID number of the client electronic document preparation terminal device and transmitting the digest value and the ID number to the external organization device; Paragraph 0060: an offline verification may automatically be performed before online verification wherein a request for verification of the time stamps for the document digest value (TS-obj, H-doc), time information (TS-obj, T-fix), and the electronic signatures (TS-obj, SIG-2) is sent to the time stamp verification server 13 at the center), and,

after the predetermined event, communicating the electronic document to the recipient data processing apparatus via the data communications network (Abstract: the document preparation terminal device 30 transmits the prepared document; Paragraph 0014: based on the configuration where a digest value generated based on an electronic document prepared by a client electronic document preparation terminal device with electronic document preparation software incorporated therein is transmitted

Art Unit: 2438

to an external organization device and the external organization device assigns the time of receipt and an electronic signature to the digest value and returns it to the client).

**Regarding claim 31**, Matsumoto discloses a computer readable medium having a program for executing a method of distributing documents to a recipient data processing device via a data communications network, the method comprising

generating an electronic document (Paragraph 0066: document preparation software installed in a terminal device at a client site, and therefore time information for certification can easily and automatically be stamped on each document during preparation of the document);

generating an original hash value from the electronic document (Paragraph 0014: a digest value computing means for computing a digest value including a hash value as a unidirectional function value based on a read document); and

communicating the original hash value to a recipient data processing apparatus before a predetermined event via a data communications network (Paragraph 0014: a transmitting means for correlating the digest value to an ID number of the client electronic document preparation terminal device and transmitting the digest value and the ID number to the external organization device; Paragraph 0060: an offline verification may automatically be performed before online verification wherein a request for verification of the time stamps for the document digest value (TS-obj, H-doc), time information (TS-obj, T-fix), and the electronic signatures (TS-obj, SIG-2) is sent to the time stamp verification server 13 at the center), and,

Art Unit: 2438

after the predetermined event, communicating the electronic document to the recipient data processing apparatus via the data communications network (Abstract: the document preparation terminal device 30 transmits the prepared document; Paragraph 0014: based on the configuration where a digest value generated based on an electronic document prepared by a client electronic document preparation terminal device with electronic document preparation software incorporated therein is transmitted to an external organization device and the external organization device assigns the time of receipt and an electronic signature to the digest value and returns it to the client).

### ***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

**8. Claims 1-9,11,19-23, 25-27, 29-30, 32 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsumoto et al. (US 2003/0159048 A1, hereinafter, Matsumoto) in view of Carro (Patent No. US 7,117,367 B2).**

**Regarding claim 1**, Matsumoto discloses a data processing system for distributing and authenticating documents from a plurality of parties to a recipient data processing apparatus, the system comprising

a plurality of document distribution devices each configured to generate an original hash value from the content of an electronic file containing a document to be distributed (Paragraph 0014: transmitting the digest value including a hash value and the ID number to the external organization device); and

a data communications network configured to communicate each of the original hash values to the recipient data processing apparatus before a predetermined event (Paragraph 0047: The electronic document preparing organization 20 fetches time data from the center each time a time stamp processing request is generated, and transmits a digest value ( hash value)for a document to be time-stamped to the center each time the time stamp processing is performed, while the center assigns time data and an electronic signature to the digest value and returns the digest value to the organization 20),

the recipient data processing apparatus configured to (Paragraph 0014: a receiving means for receiving an electronic certificate transmitted thereto from the

Art Unit: 2438

external organization device with the term of receipt and the electronic signature assigned to the digest value received by the external organization device as well as to the ID number of the client electronic document preparation terminal device):

receive the original hash values from each of the plurality of document distribution devices via the data communication network (Paragraph 0014: receiving means for receiving an electronic certificate transmitted thereto from the external organization device with the term of receipt and the electronic signature assigned to the digest value received by the external organization device as well as to the ID number of the client electronic document preparation terminal device);,

generate an original [super hash value] from the plurality of the original hash values received (Paragraph 0055: a hash value is computed for the portion "A" which is equivalent to a portion of the document to be time-stamped excluding the TS-object therefrom (a result of computing is H), and

communicate the original super hash to the plurality of document distribution devices (Paragraph 0044: a first document preparation terminal device 30 (client A) and a second document preparation terminal device 40 (client B) are connected through a communication network 50 to center),

wherein after the predetermined event, the plurality of document distribution devices are configured to (Paragraph 0054: generation of a time stamp in the first document preparation terminal device 30 as a client site, and in step S5, determination

Art Unit: 2438

is made as to whether the license is correct or not, and also as to whether the term of validity (T-BND) is within the specified term based on the system time or not)

communicate each of the respective electronic files to the recipient data processing apparatus (Abstract: the document preparation terminal device 30 transmits the prepared document),

wherein the recipient data processing apparatus is further configured to:

generate a comparative hash value from the content of the electronic file containing the document received from each of the document distribution devices (Paragraph 0059: comparison and verification of the hash value for the original time stamp information to the decoded value for the electronic signature (SIG-2)) is performed; Fig. 5),

generate a [comparative super hash value] from each of the comparative hash values (Paragraph 0050: The time stamp authenticity verifying section (for issuing inquiries to the center) has a function to compute a hash value for a document with a time stamp buried therein, a function to send and receive time stamp information verification requests and the results to and from the center, and a function to display a result of the verification).

communicate the comparative super hash value to each of the document distribution devices (Claim 5: the external organization to generate information enabling comparison and verification thereof to the electronic document to be verified at the client terminal device, and returning the generated information to the client device), and

Art Unit: 2438

determine whether or not the documents received by the recipient data processing apparatus have changed from a comparison of at least one of the original hash values and the comparative hash values, and the comparative super hash value and the original super hash value (Paragraph 0057: comparison and verification of the decoded value for the electronic signature (SIG-1) to the hash value for the original time stamp) is performed, and when it is determined that the hash value for the original time stamp information is the same as the decoded value for the electronic signature, it is displayed in step S18 that a result of the verification has not been changed after the time stamp was issued).

Matsumoto does not explicitly disclose but Carro from the same or similar fields of endeavor teaches a super hash value and a comparative super hash value that are generated from a plurality of hash values (Col. 3 lines 46-61: authenticating a text document with links to a plurality of files by modifying at least a selected attribute of invisible characters on a plurality of inter-word intervals of the text document, this method comprising the steps of: a) computing a one-way hash function of each file in order to obtain a hash value composed of a subset of hash digits for each one; Col. 8 lines 27-29: computing a one-way hash function of each file of the plurality of files to obtain a hash value composed of a subset of hash digits for each file) wherein

the hash values are compared to verify the authenticity and integrity of the document (Col. 10 lines 41-46: computing a one-way hash function of each of the files in order to obtain a new hash value for each one; and means for comparing the new

Art Unit: 2438

hash value to an origin hash value for each file  $n$  of the  $N$  files with  $n$  being 1 to  $N$  in order to authenticate a file  $n$ ).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use a super hash value and a comparative super hash value for authenticating document as taught by Carro in the teachings of Matsumoto for the advantage of authenticating a text document and the files linked thereto so that the integrity of the document and that all linked files could be checked individually, while preventing the integrity information from being separated or lost thus destroying the integrity of the document and the linked files (Col. 3 lines 46-53).

**Regarding claim 2**, the combination of Matsumoto and Carro discloses the data processing system according to claim 1, wherein the recipient data processing apparatus is configured to identify a document which has changed by comparing each original hash value with the corresponding comparative hash value, and, if the comparative hash value is not the same as the original hash value, to determine that the corresponding document has changed (Matsumoto, Paragraph 0058: when it is determined in step S17 that the hash value for the original time stamp information is not the same as the decoded value for the electronic signature (SIG-1), the system control shifts to step S19, and the second document preparation terminal device 40 displays that the result of verification has changed after the time stamp was issued).

**Regarding claim 3**, the combination of Matsumoto and Carro discloses the data processing system according to claim 1, wherein the original hash value generated by a



Art Unit: 2438

document distribution device is encrypted using a private key associated with the document distribution device (Matsumoto, Paragraph 0040-0041: Secret and public key for generation of a signature)

**Regarding claim 4**, the combination of Matsumoto and Carro discloses the data processing system according to claim 2, wherein the super hash value to be communicated to the document distribution devices is encrypted using a private key associated with the recipient data processing apparatus (Matsumoto, Paragraph 0048: hash value is a value computed through a hash function which is a unidirectional function wherein the hash function used for encryption; Paragraph 0039: Secret key for generation of a signature);

**Regarding claim 5**, the combination of Matsumoto and Carro discloses the data processing system according to claim 1, wherein the electronic file containing the document to be distributed is encrypted using a public key associated with the recipient data processing apparatus prior to being communicated to the recipient data processing apparatus (Paragraph 0057: When it is determined that the hash value is the same as (H-now), the public key-signed information encoded by the operation of the signature verification public key (K.sub.v1) for the second document preparation terminal device 40 is decoded, and based on this decoded public key-signed information, comparison and verification to the original time stamp information (T-fix, H-doc, and TSS-ID) (more specifically, comparison and verification of the decoded value for the electronic signature (SIG-1) to the hash value for the original time stamp) is performed).

**Regarding claim 6**, the combination of Matsumoto and Carro discloses the data processing system according to claim 1, wherein the predetermined event includes expiration of a time limit on a particular date (Matsumoto, Paragraph 0056: the received time information (T-fix) is checked against the term of validity (T-END) to determine whether the term or validity has been expired or not).

**Regarding claim 7**, the combination of Matsumoto and Carro discloses the data processing system as claimed in claim 1, wherein the electronic file is created by an application program (Matsumoto, Paragraph 0066: document preparation software installed in a terminal device at a client site, and therefore time information for certification can easily and automatically be stamped on each document during preparation of the document).

**Regarding claim 8**, the combination of Matsumoto and Carro discloses the data processing system as claimed in claim 7, wherein the electronic file is communicated as part of an e-mail (Matsumoto, Paragraph 0007-0008: attach the receipt with the document in electronic communication).

**Regarding claim 9**, the combination of Matsumoto and Carro discloses the data processing system as claimed in claim 7, wherein the electronic file is communicated on a portable data storage medium to the recipient data processing device via a postal service (Matsumoto, Paragraph 0007: author stores the receipt so that the author can show the receipt to a person requiring certification of the document; Paragraph 0015: A

Art Unit: 2438

computer-readable program medium for time-stamping electronic documents has a program recorded therein).

**Regarding claim 11**, the combination of Matsumoto and Carro discloses the data processing system as claimed in claim 7, wherein the document is generated from an on-line browser, and wherein the data communications network includes one of an intranet and the Internet (Matsumoto Paragraph 0044: The time stamp processing center 10 and the electronic document preparing organization 20 are connected through a communication network 50 such as the Internet to each other so that communications can be performed therebetween).

**Regarding claim 19**, Matsumoto discloses a recipient data processing device configured to authenticate documents received from one or more document distribution devices via a data communications network, the recipient data processing device comprising;

a communications interface configured to receive a plurality of original hash values from the document distribution devices via the data communication network before a predetermined event (Paragraph 0014: a transmitting means for correlating the digest value to an ID number of the client electronic document preparation terminal device and transmitting the digest value and the ID number to the external organization device; Paragraph 0060: an offline verification may automatically be performed before online verification wherein a request for verification of the time stamps for the document digest value (TS-obj, H-doc), time information (TS-obj, T-fix), and the electronic

Art Unit: 2438

signatures (TS-obj, SIG-2) is sent to the time stamp verification server 13 at the center);  
and

a data processing apparatus comprising a hashing processor configured to generate an original [super hash value] from the plurality of the received original hash values (Paragraph 0055: a hash value is computed for the portion "A" which is equivalent to a portion of the document to be time-stamped excluding the TS-object therefrom (a result of computing is H), and

communicate the original super hash value to each of the document distribution devices, wherein the data processing apparatus is configured to operate in combination with the communications interface to receive, after the predetermined event, respective electronic files from the document distribution devices (Paragraph 0014: based on the configuration where a digest value generated based on an electronic document prepared by a client electronic document preparation terminal device with electronic document preparation software incorporated therein is transmitted to an external organization device and the external organization device assigns the time of receipt and an electronic signature to the digest value and returns it to the client),

generate a comparative hash value from the content of the electronic file containing the document received from each of the distribution devices (Paragraph 0059: comparison and verification of the hash value for the original time stamp information to the decoded value for the electronic signature (SIG-2)) is performed; Fig. 5),

Art Unit: 2438

generate, using the hashing processor a [comparative super hash value] from each of the comparative hash values, communicate the comparative super hash value to the document distribution devices (Paragraph 0050: The time stamp authenticity verifying section (for issuing inquiries to the center) has a function to compute a hash value for a document with a time stamp buried therein, a function to send and receive time stamp information verification requests and the results to and from the center, and a function to display a result of the verification), and

determine whether or not the documents received by the recipient data processing apparatus have changed based a comparison of at least one of the original hash values and the comparative hash values, and the comparative super hash value and the original super hash value (Paragraph 0057: comparison and verification of the decoded value for the electronic signature (SIG-1) to the hash value for the original time stamp) is performed, and when it is determined that the hash value for the original time stamp information is the same as the decoded value for the electronic signature, it is displayed in step S18 that a result of the verification has not been changed after the time stamp was issued).

Matsumoto does not explicitly disclose but Carro from the same or similar fields of endeavor teaches a super hash value and a comparative super hash value that are generated from a plurality of hash values (Col. 3 lines 46-61: authenticating a text document with links to a plurality of files by modifying at least a selected attribute of invisible characters on a plurality of inter-word intervals of the text document, this method comprising the steps of: a) computing a one-way hash function of each file in

Art Unit: 2438

order to obtain a hash value composed of a subset of hash digits for each one; Col 8 lines 27-29: computing a one-way hash function of each file of the plurality of files to obtain a hash value composed of a subset of hash digits for each file) wherein

the hash values are compared to verify the authenticity and integrity of the document (Col. 10 lines 41-46: computing a one-way hash function of each of the files in order to obtain a new hash value for each one; and means for comparing the new hash value to an origin hash value for each file  $n$  of the  $N$  files with  $n$  being 1 to  $N$  in order to authenticate a file  $n$ ).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use a super hash value and a comparative super hash value for authenticating document as taught by Carro in the teachings of Matsumoto for the advantage of efficiently securing and verifying the authenticity of a plurality of data files, such as data files intended to be transferred over computer networks wherein digital signature of the group of files is verified, and check-values in the signature file are compared with the corresponding values computed from the data files (Col. 3 lines 11-22).

**Regarding claim 20**, the combination of Matsumoto and Carro discloses the recipient data processing apparatus as claimed in claim 19, wherein the data processing apparatus is configured to identify a document which has changed by comparing each original hash value with the corresponding comparative hash value, and if the comparative hash value is not the same as the original hash value, determine

Art Unit: 2438

that the corresponding document has changed (Matsumoto, Paragraph 0058: when it is determined in step S17 that the hash value for the original time stamp information is not the same as the decoded value for the electronic signature (SIG-1), the system control shifts to step S19, and the second document preparation terminal device 40 displays that the result of verification has changed after the time stamp was issued).

**Regarding claim 21**, the combination of Matsumoto and Carro discloses the recipient data processing apparatus as claimed in claim 19, wherein the original hash values received from the document distribution devices are encrypted using a private key associated with each document distribution device, (Matsumoto, Paragraph 0040-0041: Secret and public key for generation of a signature)and wherein

the recipient data processing apparatus comprises an encryption processor configured to decrypt the original hash values using a public key associated with the document distribution device (Matsumoto, Paragraph 0057: : the public key-signed information encoded by the operation of the signature verification public key (K.sub.v1) for the second document preparation terminal device 40 is decoded, and based on this decoded public key-signed information, comparison and verification to the original time stamp information (T-fix, H-doc, and TSS-ID) (more specifically, comparison and verification of the decoded value for the electronic signature (SIG-1) to the hash value for the original time stamp) is performed).

**Regarding claim 22**, the combination of Matsumoto and Carro discloses the recipient data processing apparatus according to claim 21, wherein the encryption

Art Unit: 2438

processor is configured to encrypt the original super hash value and the comparative super hash to be communicated to the document distribution devices in encrypted form (Matsumoto, Paragraph 0048: hash value is a value computed through a hash function which is a unidirectional function wherein the hash function used for encryption; Paragraph 0039: Secret key for generation of a signature; Claim 3: comparing and verifying the original time stamp information according to the decode public key-signed information by operating the public key for electronic signature verification at the client terminal device).

**Regarding claim 23**, the combination of Matsumoto and Carro discloses the recipient data processing apparatus according to claim 19, wherein the encryption processor is configured to decrypt the electronic file representing the distributed document using a public key associated with the document distribution devices (Matsumoto, Paragraph 0057: : the public key-signed information encoded by the operation of the signature verification public key (K.sub.v1) for the second document preparation terminal device 40 is decoded, and based on this decoded public key-signed information, comparison and verification to the original time stamp information (T-fix, H-doc, and TSS-ID) (more specifically, comparison and verification of the decoded value for the electronic signature (SIG-1) to the hash value for the original time stamp) is performed).

**Regarding claim 25**, the combination of Matsumoto and Carro discloses the recipient data processing apparatus as claimed in claim 19, wherein the communications interface includes an on-line browser facility for generating the



Art Unit: 2438

document, and wherein the data communications network includes one of an intranet and the Internet (Matsumoto Paragraph 0044: The time stamp processing center 10 and the electronic document preparing organization 20 are connected through a communication network 50 such as the Internet to each other so that communications can be performed therebetween).

**Regarding claim 26**, Matsumoto discloses a computer-implemented method for distributing documents from a plurality of parties to a recipient data processing apparatus, the method comprising:

generating, for each of the plurality of parties, an original hash value from the content of an electronic file representing a document to be distributed (Paragraph 0047: transmits a digest value (hash value) for a document to be time-stamped to the center each time the time stamp processing is performed);

communicating the original hash value to the recipient data processing apparatus before a predetermined event via a data communications network (Paragraph 0060: an offline verification may automatically be performed before online verification wherein a request for verification of the time stamps for the document digest value (TS-obj, H-doc), time information (TS-obj, T-fix), and the electronic signatures (TS-obj, SIG-2) is sent to the time stamp verification server 13 at the center);

generating, at the recipient data processing apparatus, an original [super hash value] from the plurality of the original hash values received (Paragraph 0055: a hash

Art Unit: 2438

value is computed for the portion "A" which is equivalent to a portion of the document to be time-stamped excluding the TS-object therefrom (a result of computing is H);

communicating the original super hash to the plurality of document distribution devices; and, after the predetermined event (Paragraph 0047: the center assigns time data and an electronic signature to the digest value and returns the digest value to the organization 20),

communicating, from the plurality of document distribution devices, each of the respective electronic files to the recipient data processing apparatus (Abstract: the document preparation terminal device 30 transmits the prepared document);

generating, at the recipient data processing apparatus, a comparative hash value from the content of the electronic file containing the document received from each of the distribution devices (Paragraph 0059: comparison and verification of the hash value for the original time stamp information to the decoded value for the electronic signature (SIG-2)) is performed; Fig. 5),;

generating [a comparative super hash value] from each of the comparative hash values (Paragraph 0050: The time stamp authenticity verifying section (for issuing inquiries to the center) has a function to compute a hash value for a document with a time stamp buried therein, a function to send and receive time stamp information verification requests and the results to and from the center, and a function to display a result of the verification); and

Art Unit: 2438

determining whether or not the documents received by the recipient data processing apparatus have changed based on a comparison of at least one of the original hash values and the comparative hash values, and the comparative super hash value and the original super hash value (Paragraph 0057: comparison and verification of the decoded value for the electronic signature (SIG-1) to the hash value for the original time stamp) is performed, and when it is determined that the hash value for the original time stamp information is the same as the decoded value for the electronic signature, it is displayed in step S18 that a result of the verification has not been changed after the time stamp was issued).

Matsumoto does not explicitly disclose but Carro from the same or similar fields of endeavor teaches a super hash value and a comparative super hash value that are generated from a plurality of hash values (Col. 3 lines 46-61: authenticating a text document with links to a plurality of files by modifying at least a selected attribute of invisible characters on a plurality of inter-word intervals of the text document, this method comprising the steps of: a) computing a one-way hash function of each file in order to obtain a hash value composed of a subset of hash digits for each one; Col. 8 lines 27-29: computing a one-way hash function of each file of the plurality of files to obtain a hash value composed of a subset of hash digits for each file) wherein

the hash values are compared to verify the authenticity and integrity of the document (Col. 10 lines 41-46: computing a one-way hash function of each of the files in order to obtain a new hash value for each one; and means for comparing the new

Art Unit: 2438

hash value to an origin hash value for each file  $n$  of the  $N$  files with  $n$  being 1 to  $N$  in order to authenticate a file  $n$ ).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use a super hash value and a comparative super hash value for authenticating document as taught by Carro in the teachings of Matsumoto for the advantage of authenticating a text document and the files linked thereto so that the integrity of the document and that all linked files could be checked individually, while preventing the integrity information from being separated or lost thus destroying the integrity of the document and the linked files (Col. 3 lines 46-53).

**Regarding claim 27**, the combination of Matsumoto and Carro discloses the data processing method according to claim 26, further comprising: identifying a document which has changed by comparing each original hash value with the corresponding comparative hash value, and if the comparative hash value is not the same as the original hash value, determining that the corresponding document has changed (Matsumoto, Paragraph 0058: when it is determined in step S17 that the hash value for the original time stamp information is not the same as the decoded value for the electronic signature (SIG-1), the system control shifts to step S19, and the second document preparation terminal device 40 displays that the result of verification has changed after the time stamp was issued).

**Regarding claim 29**, the combination of Matsumoto and Carro discloses the method as claimed in claim 27, further comprising: receiving from the recipient data

Art Unit: 2438

processing apparatus, an original super-hash value generated by the recipient data processing apparatus from a combination of the original hash value communicated by the data processing apparatus and a hash value generated by at least one other document distribution device (Paragraph 0014: receiving means for receiving an electronic certificate transmitted thereto from the external organization device with the term of receipt and the electronic signature assigned to the digest value received by the external organization device as well as to the ID number of the client electronic document preparation terminal device); and

receiving a comparative super hash value generated by the recipient data processing apparatus from the electronic document received from the document distribution apparatus and at least one other electronic document received from the at least one other document distribution device (Paragraph 0059: comparison and verification of the hash value for the original time stamp information to the decoded value for the electronic signature (SIG-2)) is performed; Fig. 5).

**Regarding claim 30**, Matsumoto discloses a method of authenticating documents received from a plurality of document distribution devices via a data communications network, the method comprising:

receiving a plurality of original hash values from the document distribution devices, before a predetermined events via the data communication network (Paragraph 0014: a transmitting means for correlating the digest value to an ID number of the client electronic document preparation terminal device and transmitting the digest

Art Unit: 2438

value and the ID number to the external organization device; Paragraph 0060: an offline verification may automatically be performed before online verification wherein a request for verification of the time stamps for the document digest value (TS-obj, H-doc), time information (TS-obj, T-fix), and the electronic signatures (TS-obj, SIG-2) is sent to the time stamp verification server 13 at the center);

generating an original [super hash value] from the plurality of the original hash values received (Paragraph 0055: a hash value is computed for the portion "A" which is equivalent to a portion of the document to be time-stamped excluding the TS-object therefrom (a result of computing is H);

communicating the original super hash value to each of the document distribution devices; receiving, after the predetermined event, respective electronic files from document distribution devices (Paragraph 0014: based on the configuration where a digest value generated based on an electronic document prepared by a client electronic document preparation terminal device with electronic document preparation software incorporated therein is transmitted to an external organization device and the external organization device assigns the time of receipt and an electronic signature to the digest value and returns it to the client);

generating a comparative hash value from the content of the electronic file containing the document received from each of the distribution devices (Paragraph 0059: comparison and verification of the hash value for the original time stamp

Art Unit: 2438

information to the decoded value for the electronic signature (SIG-2)) is performed; Fig. 5);

generating a [comparative super hash value] from each of the comparative hash values;

communicating the comparative super hash value to the document distribution devices (Paragraph 0050: The time stamp authenticity verifying section (for issuing inquiries to the center) has a function to compute a hash value for a document with a time stamp buried therein, a function to send and receive time stamp information verification requests and the results to and from the center, and a function to display a result of the verification); and

determining whether or not the documents received by the recipient data processing apparatus have changed based on a comparison of at least one of the original hash values, and the comparative hash value and the comparative super hash value and the original super hash value (Paragraph 0057: comparison and verification of the decoded value for the electronic signature (SIG-1) to the hash value for the original time stamp) is performed, and when it is determined that the hash value for the original time stamp information is the same as the decoded value for the electronic signature, it is displayed in step S18 that a result of the verification has not been changed after the time stamp was issued).

Matsumoto does not explicitly disclose but Carro from the same or similar fields of endeavor teaches a super hash value and a comparative super hash value that are generated from a plurality of hash values (Col. 3 lines 46-61: authenticating a text

Art Unit: 2438

document with links to a plurality of files by modifying at least a selected attribute of invisible characters on a plurality of inter-word intervals of the text document, this method comprising the steps of: a) computing a one-way hash function of each file in order to obtain a hash value composed of a subset of hash digits for each one; Col 8 lines 27-29: computing a one-way hash function of each file of the plurality of files to obtain a hash value composed of a subset of hash digits for each file) wherein

the hash values are compared to verify the authenticity and integrity of the document (Col. 10 lines 41-46: computing a one-way hash function of each of the files in order to obtain a new hash value for each one; and means for comparing the new hash value to an origin hash value for each file  $n$  of the  $N$  files with  $n$  being 1 to  $N$  in order to authenticate a file  $n$ ).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use a super hash value and a comparative super hash value for authenticating document as taught by Carro in the teachings of Matsumoto for the advantage of authenticating a text document and the files linked thereto so that the integrity of the document and that all linked files could be checked individually, while preventing the integrity information from being separated or lost thus destroying the integrity of the document and the linked files.

**Regarding claim 32,** Matsumoto discloses a computer readable medium having a program for executing a method of authenticating documents received from a plurality



Art Unit: 2438

of document distribution devices via a data communications network, the method comprising:

receiving a plurality of original hash values from the document distribution devices, before a predetermined event, via the data communication network (Paragraph 0047: transmits a digest value (hash value) for a document to be time-stamped to the center each time the time stamp processing is performed);

generating an original [super hash value] from the plurality of the original hash values received Paragraph 0055: a hash value is computed for the portion "A" which is equivalent to a portion of the document to be time-stamped excluding the TS-object therefrom (a result of computing is H);

communicating the original super hash value to each of the document distribution devices (Paragraph 0047: the center assigns time data and an electronic signature to the digest value and returns the digest value to the organization 20);

receiving, after the predetermined event, respective electronic files from document distribution devices (Abstract: the document preparation terminal device 30 transmits the prepared document);

generating a comparative hash value from the content of the electronic file containing the document received from each of the distribution devices (Paragraph 0059: comparison and verification of the hash value for the original time stamp information to the decoded value for the electronic signature (SIG-2)) is performed; Fig. 5);

Art Unit: 2438

generating a [comparative super hash value] from each of the comparative hash values Paragraph 0050: The time stamp authenticity verifying section (for issuing inquiries to the center) has a function to compute a hash value for a document with a time stamp buried therein, a function to send and receive time stamp information verification requests and the results to and from the center, and a function to display a result of the verification);

communicating the comparative super hash value to the document distribution devices (Paragraph 0047: The electronic document preparing organization 20 fetches time data from the center each time a time stamp processing request is generated, and transmits a digest value ( hash value)for a document to be time-stamped to the center each time the time stamp processing is performed, while the center assigns time data and an electronic signature to the digest value and returns the digest value to the organization 20); and

determining whether or not the documents received by the recipient data processing apparatus have changed based on a comparison of at least one of the original hash values, and the comparative hash value and the comparative super hash value and the original super hash value (Paragraph 0057: comparison and verification of the decoded value for the electronic signature (SIG-1) to the hash value for the original time stamp) is performed, and when it is determined that the hash value for the original time stamp information is the same as the decoded value for the electronic signature, it is displayed in step S18 that a result of the verification has not been changed after the time stamp was issued).

Matsumoto does not explicitly disclose but Carro from the same or similar fields of endeavor teaches a super hash value and a comparative super hash value that are generated from a plurality of hash values (Col. 3 lines 46-61: authenticating a text document with links to a plurality of files by modifying at least a selected attribute of invisible characters on a plurality of inter-word intervals of the text document, this method comprising the steps of: a) computing a one-way hash function of each file in order to obtain a hash value composed of a subset of hash digits for each one; Col. 8 lines 27-29: computing a one-way hash function of each file of the plurality of files to obtain a hash value composed of a subset of hash digits for each file) wherein

the hash values are compared to verify the authenticity and integrity of the document (Col. 10 lines 41-46: computing a one-way hash function of each of the files in order to obtain a new hash value for each one; and means for comparing the new hash value to an origin hash value for each file  $n$  of the  $N$  files with  $n$  being 1 to  $N$  in order to authenticate a file  $n$ ).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use a super hash value and a comparative super hash value for authenticating document as taught by Carro in the teachings of Matsumoto for the advantage of authenticating a text document and the files linked thereto so that the integrity of the document and that all linked files could be checked individually, while preventing the integrity information from being separated or lost thus destroying the integrity of the document and the linked files (Col. 3 lines 46-53).

**Regarding claim 34**, Matsumoto discloses a data processing apparatus for distributing documents from a plurality of parties to a recipient data processing apparatus, the apparatus comprising:

means for generating, for each of the plurality of parties, an original hash value from the content of an electronic file representing a document to be distributed (Paragraph 0014: a transmitting means for correlating the digest value to an ID number of the client electronic document preparation terminal device and transmitting the digest value and the ID number to the external organization device; Fig. 1);

means for communicating the original hash value to the recipient data processing apparatus, before a predetermined event, via a data communications network (Paragraph 0060: an offline verification may automatically be performed before online verification wherein a request for verification of the time stamps for the document digest value (TS-obj, H-doc), time information (TS-obj, T-fix), and the electronic signatures (TS-obj, SIG-2) is sent to the time stamp verification server 13 at the center);

means for generating, at the recipient data processing apparatus, an original [super hash value] from the plurality of the original hash values received values (Paragraph 0055: a hash value is computed for the portion "A" which is equivalent to a portion of the document to be time-stamped excluding the TS-object therefrom (a result of computing is H);

means for communicating the original super hash to the plurality of document distribution devices; means for communicating, after the predetermined event, from the

Art Unit: 2438

plurality of document distribution devices, each of the respective electronic files to the recipient data processing apparatus (Paragraph 0014: based on the configuration where a digest value generated based on an electronic document prepared by a client electronic document preparation terminal device with electronic document preparation software incorporated therein is transmitted to an external organization device and the external organization device assigns the time of receipt and an electronic signature to the digest value and returns it to the client);

means for generating, after the predetermined event, at the recipient data processing apparatus, a comparative hash value from the content of the electronic file containing the document received from each of the distribution devices (Paragraph 0059: comparison and verification of the hash value for the original time stamp information to the decoded value for the electronic signature (SIG-2)) is performed; Fig. 5);

means for generating, after the predetermined event, a comparative [super hash value] from each of the comparative hash values (Paragraph 0050: The time stamp authenticity verifying section (for issuing inquiries to the center) has a function to compute a hash value for a document with a time stamp buried therein, a function to send and receive time stamp information verification requests and the results to and from the center, and a function to display a result of the verification); and

means for determining whether or not the documents received by the recipient data processing apparatus have changed based on a comparison of at least one of the

Art Unit: 2438

original hash values and the comparative hash values, and the comparative super hash value and the original super hash value (Paragraph 0057: comparison and verification of the decoded value for the electronic signature (SIG-1) to the hash value for the original time stamp) is performed, and when it is determined that the hash value for the original time stamp information is the same as the decoded value for the electronic signature, it is displayed in step S18 that a result of the verification has not been changed after the time stamp was issued).

Matsumoto does not explicitly disclose but Carro from the same or similar fields of endeavor teaches a super hash value and a comparative super hash value that are generated from a plurality of hash values (Col. 3 lines 46-61: authenticating a text document with links to a plurality of files by modifying at least a selected attribute of invisible characters on a plurality of inter-word intervals of the text document, this method comprising the steps of: a) computing a one-way hash function of each file in order to obtain a hash value composed of a subset of hash digits for each one; Col. 8 lines 27-29: computing a one-way hash function of each file of the plurality of files to obtain a hash value composed of a subset of hash digits for each file) wherein

the hash values are compared to verify the authenticity and integrity of the document (Col. 10 lines 41-46: computing a one-way hash function of each of the files in order to obtain a new hash value for each one; and means for comparing the new hash value to an origin hash value for each file  $n$  of the  $N$  files with  $n$  being 1 to  $N$  in order to authenticate a file  $n$ ).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use a super hash value and a comparative super hash value for authenticating document as taught by Carro in the teachings of Matsumoto for the advantage of efficiently securing and verifying the authenticity of a plurality of data files, such as data files intended to be transferred over computer networks wherein digital signature of the group of files is verified, and check-values in the signature file are compared with the corresponding values computed from the data files (Col. 3 lines 11-22).

**9. Claims 10 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsumoto in view of Carro as applied to claim 1 and 19 above, and further in view of Zhao (US 2002/0122568 A1).**

**Regarding claim 10**, the combination of Matsumoto and Carro does not explicitly disclose but Zhao from the same or similar fields of endeavor teaches that the data processing system as claimed in claim 9, wherein

the original hash value is represented as a bar code, the bar code being arranged in association with the portable data storage medium, and wherein the recipient data processing apparatus includes a storage medium reader configured to reproduce the electronic file from the portable data storage medium, and a bar code reader for reproducing the original hash value from the bar code associated with the portable data storage medium, the electronic file representing the document being

Art Unit: 2438

stored in association with the hash value in a data store (Paragraph 0056: semantic digest 207 is a visible bar code wherein semantic digest 207 may include additional information; for example, it may be encrypted and semantic digest 207 may include an identifier for the user whose public key is required to decrypt semantic digest 207).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have bar code reader corresponding to hash value as taught by Zhao in the teachings of Matsumoto and Carro for the advantage of providing improved techniques for distributing digital representations (Paragraph 0020).

**Regarding claim 24**, the combination of Matsumoto and Carro does not explicitly disclose but Zhao from the same or similar fields of endeavor teaches the recipient data processing apparatus according to claim 19, comprising a data storage medium reader configured to reproduce the electronic file from the portable data storage medium, and a bar code reader for reproducing the original hash value from the bar code associated with the portable data storage medium, the electronic file representing the document being stored in association with the .hash value in a data store (Paragraph 0056: semantic digest 207 is a visible bar code wherein semantic digest 207 may include additional information; for example, it may be encrypted and semantic digest 207 may include an identifier for the user whose public key is required to decrypt semantic digest 207).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have bar code reader corresponding to hash value as taught by



Art Unit: 2438

Zhao in the teachings of Matsumoto and Carro for the advantage of providing improved techniques for distributing digital representations (Paragraph 0020).

**10. Claims 13 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsumoto as applied to claim 12 above in view of Carro (Patent No. US 7, 117, 367 B2).**

**Regarding claim 13**, Matsumoto does not explicitly disclose but Carro from the same or similar fields of endeavor teaches the document distribution device as claimed in claim 12, wherein the data processing apparatus is configured to receive from the recipient data processing apparatus, via the communications interface, an original [super-hash value] generated by the recipient data processing apparatus from a combination of the original hash value communicated by the data processing apparatus and a hash value generated by at least one other document distribution device (Col. 10 lines 41-46: computing a one-way hash function of each of the files in order to obtain a new hash value for each one; and means for comparing the new hash value to an origin hash value for each file n of the N files with n being 1 to N in order to authenticate a file n); and

to receive a comparative [super hash value] generated by the recipient data processing apparatus from the electronic document received from the document distribution device and at least one other electronic document received from the at least one other document distribution device (Col. 3 lines 46-61: authenticating a text

Art Unit: 2438

document with links to a plurality of files by modifying at least a selected attribute of invisible characters on a plurality of inter-word intervals of the text document, this method comprising the steps of: a) computing a one-way hash function of each file in order to obtain a hash value composed of a subset of hash digits for each one; Col 8 lines 27-29: computing a one-way hash function of each file of the plurality of files to obtain a hash value composed of a subset of hash digits for each file).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use a super hash value and a comparative super hash value for authenticating document as taught by Carro in the teachings of Matsumoto for the advantage of authenticating a text document and the files linked thereto so that the integrity of the document and that all linked files could be checked individually, while preventing the integrity information from being separated or lost thus destroying the integrity of the document and the linked files (Col. 3 lines 46-53).

**Regarding claim 15**, Matsumoto does not explicitly disclose but Carro from the same or similar fields of endeavor teaches the document distribution device as claimed in claim 14, wherein the data processing apparatus is configured to decrypt [the super hash value] received from recipient data processing apparatus using a private key associated with the recipient data processing apparatus (Col. 3 lines 46-61: authenticating a text document with links to a plurality of files by modifying at least a selected attribute of invisible characters on a plurality of inter-word intervals of the text

Art Unit: 2438

document, this method comprising the steps of: a) computing a one-way hash function of each file in order to obtain a hash value composed of a subset of hash digits for each one; Col. 8 lines 27-29: computing a one-way hash function of each file of the plurality of files to obtain a hash value composed of a subset of hash digits for each file).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use a super hash value and a comparative super hash value for authenticating document as taught by Carro in the teachings of Matsumoto for the advantage of authenticating a text document and the files linked thereto so that the integrity of the document and that all linked files could be checked individually, while preventing the integrity information from being separated or lost thus destroying the integrity of the document and the linked files (Col. 3 lines 46-53).

**11. Claims 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsumoto as applied to claim 12 above in view of Zhao (US 2002/0122568 A1).**

**Regarding claim 17**, Matsumoto discloses the document distribution device as claimed in claim 16, wherein the communications interface includes a recording device configured to record the electronic file on a portable data storage medium, a bar code generator operable to represent the original hash value as a bar code, and wherein the communications interface is configured to associate the bar code with the portable data storage medium (Paragraph 0056: semantic digest 207 is a visible bar code wherein

Art Unit: 2438

semantic digest 207 may include additional information; for example, it may be encrypted and semantic digest 207 may include an identifier for the user whose public key is required to decrypt semantic digest 207).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have bar code reader corresponding to hash value as taught by Zhao in the teachings of Matsumoto and Carro for the advantage of providing improved techniques for distributing digital representations (Paragraph 0020).

### ***Conclusion***

**12.** The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Harrison et al. US 2002/0026583 A1 discloses document transmission techniques IV.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MAHFUZUR RAHMAN whose telephone number is (571)270-7638. The examiner can normally be reached on Monday thru Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T. Arani can be reached on (571) - 272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2438

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R./

Examiner, Art Unit 2438

/Taghi T. Arani/

Supervisory Patent Examiner, Art Unit 2438